IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHWESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 14-5023-01-CR-SW-BP
	)	
MARK EUGENE DREW,	)	
	)	
Defendant.	)	

REPORT AND RECOMMENDATION OF U.S. MAGISTRATE JUDGE

Pursuant to 28 U.S.C. § 636(b), the above-styled criminal action was referred to the undersigned for preliminary review. Defendant Drew filed a Motion to Suppress Evidence and Request for a *Franks* Hearing in this matter. (Doc. 22.) Defendant contends that any evidence seized and statements derived directly or indirectly from items seized by law enforcement pursuant to a search warrant issued on November 21, 2013 should be suppressed.[1] The Court held a hearing on the Motion on August 6, 2015. (*See* Doc. 38.) Defendant was present with his attorney, David Mercer. The United States was represented by James J. Kelleher. For the reasons set forth below, it is hereby **RECOMMENDED** that the Motion to Suppress Evidence, (Doc. 22), be **DENIED**.

I. Findings of Fact[2]

During the hearing on August 6, the Court received evidence and heard testimony from the parties. Special Agent Elizabeth Weiland of the FBI testified that through her role as

[1] The specific items or statements Defendant seeks to suppress are: (1) an EMachine desktop computer, Model W5333, Serial Number CGM7630008155; (2) a Gateway desktop computer, Model 510X, Serial Number 1099965470; (3) an EMachine desktop computer, Model D4362, Serial Number GV24410000881; (4) a Sandisk 4 GB USB flash drive; (5) various CD or DVD disks seized from the home of Mark Drew; and (5) all statements allegedly made by Mark Drew on November 21, 2013 or thereafter.

[2] The facts set forth herein are taken from the testimony adduced at the hearing on the instant Motion and the exhibits admitted during the hearing. A hearing transcript appears as Doc. 41, and the parties' exhibit lists appear as Docs. 39 and 40.

member of the Crimes Against Children Squad, she received information from an international taskforce that they were investigating a Russian citizen who uploaded child pornography. The same international task force informed Agent Weiland that they believed that Russian citizen was using a certain website to exchange child pornography with other individuals ("Website A"), and brought her attention to a user "maddog8in." Maddog8in was active on the website between 2008 and 2012. During that time, maddog8in posted several comments to photos, the most recent in August 2012, and also uploaded a total of 29 photographs in three albums. Of those 29 photographs posted, the FBI came to believe that five of those images contained child pornography.[3] Of those five photographs, Agent Weiland testified as to two. In both of those photographs, Agent Weiland testified that the child was bottomless from the waist down and that the outline of the pubic and upper vaginal area was visible. She noted, however, that the child's legs were not open.

Agent Weiland testified that maddog8in had been kicked off Website A in 2012 for posting copyrighted images. However, a user with the same internet protocol ("IP") address[4] as maddog8in signed up for Website A using the name "maddog7." Agent Weiland then testified that the FBI took steps to identify maddog8in with the email address he used to register with Website A (maddog8in@yahoo.com). The FBI sent an administrative subpoena to Yahoo!, seeking information regarding that email address. The response to the subpoena identified two IP addresses associated with maddog8in's email (69.55.132.66 and 24.119.190.79), one of which

[3] The way in which the FBI identifies and tracks photographs containing child pornography is somewhat technical. Essentially, an image is converted into a unique number that becomes associated with and identifies that exact image through a mathematic formula. That number is called the "hash value." The FBI and other international agencies maintain databases with the hash values for images the agency knows contain child exploitation materials. When trying to ascertain whether an image contains child pornography, the FBI runs images (such as the ones uploaded on Website A) through these databases to see if the hash values of those images match with other images known to contain child exploitation materials. Using this method, the FBI concluded that five photographs uploaded by maddog8in had hash values matching photographs containing child pornography.

[4] An IP address is a unique address assigned to an individual by their internet service provider.

was connected to an individual in Missouri with Cable One as the internet service provider (24.119.190.79). Agent Weiland testified that the FBI also subpoenaed Cable One seeking subscription information. In response to that subpoena, Cable One provided the name Mark Drew and the address of 3030 South Oliver Avenue in Joplin, Missouri. Agent Weiland then notified another division of the FBI of these findings and sent Chip Root, Detective for the Joplin Police Department and Task Force Officer ("TFO") for the FBI Child Exploitation Task Force, a disk of information regarding the activity of maddog8in on Website A. Agent Weiland testified that the investigation into Website A has led to approximately 30 prosecutions for crimes involving child pornography.

Chip Root also testified for this hearing. He testified that, upon receiving the disk containing information regarding maddog8in and the associated IP address in 2013, he contacted Agent Weiland to discuss the investigation. He then began conducting surveillance on 3030 South Oliver Avenue in Joplin, Missouri. Based on the information contained on the disk and his surveillance, TFO Root authored and swore an affidavit supporting a search warrant for 3030 South Oliver Avenue in Joplin, Missouri. Generally, TFO Root's affidavit explained where the data regarding maddog8in and Website A came from, how TFO Root obtained that data, and what steps the investigators took in order to lead to Mark Drew and 3030 South Oliver Avenue in Joplin, Missouri. As is relevant to the instant Motion, the affidavit stated the following:[5]

> 32. On October 7, 2013, the Affiant initiated an investigation into a subject believed be living in the city of Joplin, Missouri, using the online screen name of "maddog8in." This user is suspected of uploading suspected child sexual exploitation images to a website, hereafter referred to as "Website A" to protect the integrity of the investigation, via the internet.
>
> 33. Website A is an image sharing website that is hosted outside the United States. It is a free website. Website A is organized by different forums according to topic. Examples

[5] A complete copy of the search warrant and accompanying affidavit was admitted into evidence as Government's Exhibit 6. (*See* Doc. 39, Government's Exhibit Index.)

include topics such as “architecture,” “travel,” “family,” and “autos.” Each website forum contains albums posted and named by the registered website user that created the album.

34. To register an account, and become a “member” of Website A, a user must provide a valid email address in order to receive a password provided by Website A. The user must create a new username and password as a login, and as a member, may create albums and post images within the albums. Each album is listed under their username and can be made available to all individuals on the web or make an album password protected, that is only accessible to individuals who know or have the password. Using a password protected album, a member may post preview pictures that may be viewed without a password, while the password-protected portion contains additional images that are only visible using the password. Individuals viewing the images are able to post comments about the images and the user can respond to the comments being posted.

35. Website A, has become popular with individuals seeking to post and/or download child sexual exploitation images, in particular through the “nudity” and “kids” forums. Examples of the names of albums law enforcement has observed with these two forums include “13 yo boy pies,” “street boys,” “Cute little brunette,” “Baby and Toddler Boys,” and “Maria cute chubby 16 yo (nude) (password protected).”

36. U.S. law enforcement has observed that some, but not all of Website A’s albums contain child pornography, which is most often found in password protected albums. While most of the images law enforcement has seen posted in the public preview portion of these albums may not constitute child pornography, often evidence from the images, and comments posted about the album by other individuals as well as the member who created the album, indicates that the particular poster or person who created the album has a sexual interest in children and that these individual's interest in Website A lies in the ability to meet other individuals with a sexual interest in children.

37. Since November 2010, Department of Justice Child Exploitation and Obscenity Section (CEOS) High Technology Investigative Unit (HTIU) has been involved in the investigation of over two dozen Website A users who either post sexually explicit images of children to Website A or distributed sexually explicit images of children to another user to obtain their password. In over half of these cases, investigation revealed that these individuals were actively molesting children and/or posting images of that abuse of Website A.

38. On July 22, 2013, Website A user “maddog8in” was identified as creating albums and posting them to Website A. The e-mail address associated with user “maddog8in” was listed as “maddog8in@yahoo.com.” “maddog8in” was found to have posted three albums. The first album was named, “24 yo daughter & friend” with an album description of “please leave comments trade with other dads” and advertised 12 photos inside the album. The second album was titled, “daughter in shower and friend,” with an album description of “love to trade p4p with other dads” and also advertised 12 photos inside the album. The third album was titled, “Santas Elves.” This album did not have an album description but advertised five photos. It was noted that user id “maddog8in” commented

13 times on various images examples of the comments are as follows: "Love to see more of her love to trade on yahoo." Posted on 03/24/2009 at 21:28:05 UTC. "Nice set check mine out and would love to trade pass." Posted on 01/29/2010 at 13:13:26 UTC. "Lily what a sexy lady what part of OK are you from in MO here would love to chat some time check out my albums." Posted on 11/29/2011 at 01:29:02 UTC. Etc.

39. On February 12, 2013, an administrative subpoena was sent to Yahoo! regarding e-mail address, "maddog8in@yahoo.com" requesting subscriber information for this user. On February 27, 2013, Yahoo! provided the following subscriber information: Name: Mr Mad Dog, login Name: "maddog8in@grouply.com;" Alternate E-mail: "maddog8in@grouply.com." Account Created: IP address 69.55.132.66 on June 11, 2006 at 11:51:59 GMT. Account status: Active. Last login IP: 24.119.190.79 on February 26, 2013 at 01:45:12 GMT.

40. On March 19, 2013 an administrative subpoena was served on Cable One Inc. requesting subscriber information for IP address 24.119.190.79 from January 14, 2013 at 12:02:13 GMT to February 26, 2013 at 01:45:12 GMT. On March 25, 2013, Cable One Inc. provided the following subscriber information for the above listed IP address. Account holder: Mark Drew, Address: 3030 S. Oliver Ave., Joplin, MO 64804 with phone number 417-623-6861.

41. On October 7, 2013, the Affiant reviewed a compact disc containing image files posted by Website A user "maddog8in" to said website. The five images depict the same female child; that appears to be approximately 13 years old. The images depict the child in various forms of undress and posing suggestively for the camera. Four of the five images have the name, "Laura" in the title. One of the images titled, "Laura_serie2_030" depicts the child lying on a couch with her arms over her head. She is naked from the waist down and a large birth mark is visible on her left hip. Her leg is crossed over herself, preventing full view of her vagina in this preview photo. The Affiant reviewed the associated comments posted to these albums. The dates of the comments were between November 2008 and August 2012. An example of the comments: are: 2008-11-03 at 09:08:24 from user ID "maddog8in," "love to trade with other dads." 2008-11-05 at 17:44:15, "wooooooow!!! Your daughter's tits are great!, have you seen her pussy?"; 2011-10-18 at 13:11:40, "The vids from Laura when younger are nicer;)."

(*See* Doc. 39, Government's Exhibit 6, ¶¶ 32-41.) TFO Root further testified that he did not issue an administrative subpoena for the IP address 69.55.132.66, which appears in ¶ 39 of his affidavit, and, as a result, testified that that IP address was never linked to Mark Drew.

The undersigned signed and issued the warrant on November 13, 2013 authorizing the search of 3030 South Oliver Avenue in Joplin, Missouri and seizure of items related to the production, receipt, distribution, and possession of child pornography. (*See generally* Doc. 39,

Government's Exhibit 6.) The warrant was executed on November 21, 2013. Law enforcement officers seized three computers, a flash drive, and a DVD, which collectively contained a total of 351 images depicting child pornography. Defendant was subsequently charged with the receipt and distribution of child pornography.

II. Discussion

Defendant makes three arguments in support of his Motion. First, Defendant contends that the affidavit for the search warrant contained false or misleading statements or material omissions made knowingly or recklessly such that, absent the false or misleading statements, the affidavit lacks probable cause. *See Franks v. Delaware*, 438 U.S. 154 (1978). Second, Defendant generally contends that the affidavit did not contain adequate probable cause to support the issuance of a search warrant. Third, Defendant argues that the affidavit is based upon information obtained through administrative subpoenas that violate the Fourth Amendment. The Court takes up each argument below.

a. *Franks* Allegations

The Fourth Amendment requires that a search warrant be issued only upon a showing of probable cause. *United States v. Williams*, 477 F.3d 554, 557 (8th Cir. 2007). In order to challenge a finding of probable cause under *Franks*, a defendant must show, by a preponderance of the evidence, that: (1) in preparing the affidavit supporting the search warrant, the affiant deliberately and knowingly, or with reckless disregard for the truth, included falsehoods; and (2) the affidavit, if supplemented by the omitted information, could not support a finding of probable cause. *Franks*, 438 U.S. at 171-72. An evidentiary hearing on an alleged *Franks* violation is not warranted unless a Defendant makes a strong initial showing of that a deliberate falsehood or of reckless disregard for the truth. *See United States v. Hollis*, 245 F.3d 671, 673 (8th Cir. 2001)

(citing *Franks*, 438 U.S. at 170-71) ("Although a search warrant affidavit is presumed to be valid, a defendant may obtain a hearing on the validity of the warrant by making a substantial preliminary showing that the affidavit contains a material statement by the affiant which is deliberately false or which was made with reckless disregard for the truth.").

Here, Defendant first contends that the affiant, TFO Root, intentionally or recklessly omitted information that the FBI investigation was based in part on information provided to the agency by foreign law enforcement agencies and employees of Website A, and that these sources were completely unreliable. Second, Defendant argues that TFO Root intentionally or recklessly omitted information from his affidavit showing that the connection between Website A and 3030 South Oliver Avenue in Joplin, Missouri was incomplete, had a high risk of taint or corruption, or lacked reliability. Third, Defendant argues that TFO Root failed to share information showing a strong possibility of corruption and compromise due to another user having a connection with the images at issue. Lastly, Defendant contends that TFO Root intentionally or recklessly made false or misleading impression that the female child's genitalia were partially visible in some of the images. Based only on this last argument, the Court concluded that Defendant had made a strong initial showing of a deliberate falsehood or of reckless disregard for the truth with regard to the description of the photograph and thus conducted a hearing on this matter. *See Hollis*, 245 F.3d at 673.

With regards to Defendant's first argument, the Court concludes that it is without merit. Defendant argues that, because the FBI became aware of Website A through a Russian citizen involved with the site and foreign law enforcement agencies investigating him, the information in the affidavit regarding Website A came from unreliable sources. However, the evidence of record shows that the FBI's independent investigation into Website A and its connection to the

production and distribution of child pornography corroborated the information that came from those sources. The affidavit similarly states that some of the albums posted on Website A contained child pornography. Further, it states that the FBI's investigation of Website A led to further investigation of approximately 24 individuals using the site, which led to the discovery that half of those individuals were actively molesting children and/or posting images of that abuse. Because this information regarding Website A was independently corroborated by an FBI investigation, which is explicitly discussed in the affidavit, the Court cannot conclude that TFO Root made intentional or reckless statements or omissions regarding the reliability of the original sources. Therefore, Defendant's first argument fails.

As to Defendant's second and third arguments, Defendant presented no evidence that TFO Root made any intentional or reckless omissions in his affidavit regarding those issues. Defendant did not present any evidence indicating that the connections between Website A and 3030 South Oliver Avenue in Joplin, Missouri were incomplete, had a high risk of taint, or lacked of reliability. Nor did Defendant make any showing that another user corrupted or compromised the images that led the investigation to him. Defendant did present evidence showing that an administrative subpoena was not sent for the IP address 69.55.132.66, which appears in ¶ 39 of TFO Root's affidavit. However, the affidavit clearly states that two IP addresses were associated with the email maddog8in@yahoo.com. It then states that an administrative subpoena was sent with regard to the one of those IP addresses (24.119.190.79). The fact that the affidavit is silent as to the second IP address is not a material omission. Nothing in the affidavit indicated that the FBI did anything further with the second IP address, and the affidavit is not deficient for failing to state the FBI did not issue a subpoena regarding that IP address. The affidavit indicated that the FBI chose to pursue the IP address with the most

recent activity, which, as discussed below, was sufficient to establish probable cause in this case. As such, Defendant has not shown that TFO Root made any such omissions intentionally or with reckless disregard for the truth. Thus, Defendant's second and third arguments fail.

Defendant last contends that the affidavit intentionally or with reckless disregard for the truth created the false and misleading impression that the comments on the website were associated with the images described in ¶ 41 of the affidavit. Specifically, Defendant argues that the affidavit misled the Court to believe that the female child's genitalia were partially visible in those images. However, the Court was not given that impression by the language provided in ¶ 41. Instead, when reviewing that section of the affidavit, the Court understood it to mean that the child's genitalia were not fully visible, but rather were obscured due to the positioning of the child's legs. Additionally, Agent Weiland testified that, though her genitalia were obscured, the upper part of the child's vaginal region was visible in these photographs. The photographs of the child, which were admitted into evidence during the hearing on this matter, corroborate Agent Weiland's characterization of the child's positioning. Moreover, the affidavit does not give the false or misleading impression that the comments were connected to the specific photos in the albums. Rather, it states that comments by maddog8in were posted to the albums generally, and then provides examples of those comments. (*See* Doc. 39, Government's Exhibit 6, ¶ 41.) Given the evidence of record, the Court cannot conclude that TFO Root intentionally or recklessly made false or misleading statements regarding the photographs in ¶ 41.

Considering the record as a whole, Defendant has failed to show by a preponderance of the evidence that the affidavit contains intentional or reckless false or misleading statements. Therefore, the Court concludes that no *Franks* violation occurred in this case.[6]

b. Probable Cause

In addition to arguing that TFO Root made intentional or reckless false statements in the affidavit supporting the warrant, Defendant contends that the warrant is generally not supported by probable cause. "Probable cause exists when there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Scott*, 610 F.3d 1009, 1013 (8th Cir. 2010) (internal marks and quotations omitted). A court determines whether probable cause exists by looking at the totality of the circumstances. *United States v. Williams*, 10 F.3d 590, 593 (8th Cir. 1993). In analyzing a warrant issued upon the supporting affidavit, "only th[e] information which is found within the four corners of the affidavit may be considered in determining the existence of probable cause." *United States v. Solomon*, 432 F.3d 824, 827 (8th Cir. 2005) (quotation omitted). Further, a court should examine affidavits supporting warrants "under a common sense approach and not in a hypertechnical fashion." *Williams*, 10 F.3d at 593.

Here, the affidavit provided sufficient information to establish probable cause. Specifically, the affidavit explained that someone using the username maddog8in, who was active on Website A between 2008 and 2012, had posted photographs containing child pornography onto Website A. The affidavit further outlined that, based on that information, the FBI issued a subpoena seeking information regarding maddog8in's email address in February 2013. The response to that subpoena revealed that an active subscriber had last logged into that

[6] Because the Court concludes that the affidavit did not contain false or misleading statements made intentionally or with reckless disregard for the truth, the Court need not proceed to the second prong of the *Franks* test to analyze whether probable cause would have existed without those statements.

account at the IP address 24.119.190.79. The affidavit then explained that another subpoena was issued seeking information regarding that IP address. The information provided associated IP address 24.119.190.79 with an internet service subscriber named Mark Drew and the address of 3030 South Oliver Avenue in Joplin, Missouri. Based on a common sense approach, the Court concludes that this information was sufficient to show a fair probability that evidence of a crime involving child pornography would be found at 3030 South Oliver Avenue in Joplin, Missouri.

Defendant also takes issue with the lapse in time between events in this case. That is, Defendant argues that the information in the affidavit is "fatally stale" and thus lacks probable cause because a significant amount of time passed between when the postings on Website A were made, when the subpoenas were issued and the information returned, and when the affidavit was made and the search warrant was executed.[7] "The date of the occurrence of the facts relied upon in an affidavit is of importance in the determination of probable cause because untimely information may be deemed stale." *United States v. Summage*, 481 F.3d 1075, 1078 (8th Cir. 2007) (citation omitted). However, staleness is not determined by a bright-line test, but rather is "examined in the context of the specific case and the nature of the crime under the investigation." *Id.* (quotation omitted). Here, TFO Root stated that in his experience investigating child pornography cases "[c]omputer files or remnants of such files [containing child pornography] can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet." (*See* Doc. 39, Government's Exhibit 6, ¶¶ 24, 28.) That information, TFO Root's testimony, and the fact that the IP address associated with Defendant's address was active were sufficient to create a fair probability that a search of 3030 South Oliver Avenue in Joplin, Missouri would reveal evidence of a crime involving child

[7] Approximately fifteen months passed between maddog8in's last activity on Website A, a comment in August 2012, and the execution of the search warrant in November 2013.

pornography. *See United States v. Lemon*, 590 F.3d 612, 615 (8th Cir. 2010) (noting that it "is not a new revelation" that pedophiles do not quickly dispose of child pornography, and holding the eighteenth month interim lapse did not render the information stale); *see also Summage*, 481 F.3d at 1078 (when timeline of events was not included in the affidavit, "it could be presumed that [the defendant] would maintain in his possession the video and photographs [containing child pornography] that he made[.]")

Even if the Court were to conclude that the warrant was not supported by probable cause or that the information in the affidavit was fatally stale, the *Leon* good faith exception would apply in this case. Though a violation of Fourth Amendment would usually result in the suppression of the evidentiary fruits of the illegal search, *see United States v. Riesselman*, 646 F.3d 1072, 1078 (8th Cir. 2011), this exclusionary rule is not applied "when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *United States v. Leon*, 468 U.S. 897, 920 (1984). As relevant here, there are two situations wherein an officer's reliance on a warrant would not be in good faith. First, the exception does not apply "when the affidavit or testimony supporting the warrant contained a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge." *United States v. Proell*, 485 F.3d 427, 431 (8th Cir. 2007). Second, the exception does not apply "when the affidavit in support of the warrant is so lacking in indicia of probable cause as to render official belief in its existence *entirely unreasonable*." *Id.* (emphasis original, internal quotation and marks omitted).[8] As previously discussed, neither of those circumstances applies in this case. There is no evidence that TFO Root made knowing, intentional, or reckless false statements; further, the affidavit was not so devoid of information that the officers should have concluded that that no probable cause existed. Rather, the evidence

[8] Defendant only argues *Leon* does not apply because of these two circumstances.

of record generally shows that the officers searched 3030 South Oliver Avenue in good faith reliance on the search warrant issued by the undersigned. As such, the fruits of the search in this case need not be suppressed. *See, e.g., United States v. Rugh*, 968 F.2d 750, 753-54 (8th Cir. 1992) (good faith exception applied when warrant contained sixteenth month old information that a suspect possessed child pornography because pedophiles tend to retain such materials for long periods of time).

c. Administrative Subpoenas

Defendant last argues that the administrative subpoenas, which revealed information regarding maddog8in's email and IP address, intruded into Defendant's private personal digital and information without general reasonableness. The Court notes that Defendant presented no evidence regarding this issue at the hearing. Additionally, the Court need not address whether general reasonableness existed to support the issuance of these subpoenas because Defendant does not have a reasonable expectation of privacy to subscriber information provided to an internet provider under the Fourth Amendment. *See United States v. Wheelock*, 772 F.3d 825, 828-29 (8th Cir. 2014). Thus, a warrant was not necessary to obtain that information. *Id.* at 829 ("Because [the defendant] had no reasonable expectation of privacy in the subscriber information, a warrant was not necessary.") (citation omitted). As such, Defendant's argument regarding the administrative subpoenas fails.

III. Conclusion

Therefore, based on all the foregoing, and pursuant to 28 U.S.C. § 636(b) and Local Rule 72.1 of the United States District Court for the Western District of Missouri, the undersigned hereby **RECOMMENDS** that Defendant's Motion to Suppress, (Doc. 22), be **DENIED**.

IT IS SO ORDERED.

/s/ *David P. Rush*
DAVID P. RUSH
UNITED STATES MAGISTRATE JUDGE

DATE: September 10, 2015